

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

- 1 1. (Currently amended) A method to facilitate global timeout in a
2 distributed computing environment, comprising:
3 receiving an access request from a user at an application in the distributed
4 computing environment;
5 determining if the distributed computing environment has issued an
6 authentication to a user device through which the user accesses the application,
7 wherein the authentication is stored within a time-stamped token on the user-
8 device, and ~~wherein determining if~~ the authentication has not expired by
9 comparing a time within the time-stamped token against a current time; and
10 if the authentication has not been received or has expired, redirecting the
11 access request to a single sign-on server for the distributed computing
12 environment;
13 otherwise granting access to the application to the user.
- 1 2. (Original) The method of claim 1, wherein the distributed
2 computing environment includes multiple partner applications distributed across
3 multiple network servers coupled to a public network.
- 1 3. (Original) The method of claim 2, wherein the public network
2 includes the Internet.

1 4. (Currently amended) The method of ~~claim 2~~claim 1, wherein
2 determining if the distributed computing environment has issued the
3 authentication to the user involves:
4 receiving an authentication credential from the user;
5 verifying that the authentication credential is valid; and
6 providing the time-stamped token to the user-device, wherein the time-
7 stamped token includes the authentication and a time.

1 5. (Original) The method of claim 4, wherein determining if the
2 authentication has expired involves:
3 recovering the time-stamped token from the user-device;
4 adding the specified period to the time within the time-stamped token to
5 produce an expiry time; and
6 detecting if a current time is later than the expiry time, whereby if the
7 current time is later than the expiry time, the authentication has expired.

1 6. (Original) The method of claim 5, wherein the time within the
2 time-stamped token is updated to the current time by a partner application when
3 the partner application is accessed.

1 7. (Original) The method of claim 4, wherein the time-stamped token
2 is a domain cookie, wherein the domain cookie is accessible by multiple network
3 servers within a domain on the public network.

1 8. (Original) The method of claim 4, wherein the time-stamped token
2 is encrypted to prevent attacks.

1 9. (Currently amended) A computer-readable storage medium storing
2 instructions that when executed by a computer cause the computer to perform a
3 method to facilitate global timeout in a distributed computing environment,
4 | wherein the computer readable storage medium includes one of a volatile memory
5 | and a non-volatile memory, the method comprising:
6 receiving an access request from a user at an application in the distributed
7 computing environment;
8 determining if the distributed computing environment has issued an
9 authentication to a user device through which the user accesses the application,
10 wherein the authentication is stored within a time-stamped token on the user-
11 | device, and ~~wherein determining if the authentication has not expired by~~
12 | comparing a time within the time-stamped token against a current time; and
13 if the authentication has not been received or has expired, redirecting the
14 access request to a single sign-on server for the distributed computing
15 environment;
16 otherwise granting access to the application to the user.

1 10. (Original) The computer-readable storage medium of claim 9,
2 wherein the distributed computing environment includes multiple partner
3 applications distributed across multiple network servers coupled to a public
4 network.

1 11. (Original) The computer-readable storage medium of claim 10,
2 wherein the public network includes the Internet.

1 12. (Currently amended) The computer-readable storage medium of
2 | ~~claim 10~~claim 9, wherein determining if the distributed computing environment
3 | has issued the authentication to the user involves:

4 receiving an authentication credential from the user;
5 verifying that the authentication credential is valid; and
6 providing the time-stamped token to the user-device, wherein the time-
7 stamped token includes the authentication and a time.

1 13. (Original) The computer-readable storage medium of claim 12,
2 wherein determining if the authentication has expired involves:
3 recovering the time-stamped token from the user-device;
4 adding the specified period to the time within the time-stamped token to
5 produce an expiry time; and
6 detecting if a current time is later than the expiry time, whereby if the
7 current time is later than the expiry time, the authentication has expired.

1 14. (Original) The computer-readable storage medium of claim 13,
2 wherein the time within the time-stamped token is updated to the current time by a
3 partner application when the partner application is accessed.

1 15. (Original) The computer-readable storage medium of claim 12,
2 wherein the time-stamped token is a domain cookie, wherein the domain cookie is
3 accessible by multiple network servers within a domain on the public network.

1 16. (Original) The computer-readable storage medium of claim 12,
2 wherein the time-stamped token is encrypted to prevent attacks.

1 17. (Currently amended) An apparatus to facilitate global timeout in a
2 distributed computing environment, comprising:
3 a receiving mechanism that is configured to receive an access request from
4 a user at an application in the distributed computing environment;

5 a determining mechanism that is configured to determine if the distributed
6 computing environment has issued an authentication to a user device through
7 which the user accesses the application, wherein the authentication is stored
8 within a time-stamped token on the user-device, and ~~wherein~~ determine if the
9 authentication has not expired by comparing a time within the time-stamped token
10 against a current time; and
11 a redirecting mechanism that is configured to redirect the access request to
12 a single sign-on server for the distributed computing environment if the
13 authentication has not been received or has expired.

1 18. (Original) The apparatus of claim 17, wherein the distributed
2 computing environment includes multiple partner applications distributed across
3 multiple network servers coupled to a public network.

1 19. (Original) The apparatus of claim 18, wherein the public network
2 includes the Internet.

1 20. (Currently amended) The apparatus of ~~claim 18~~ claim 17, wherein
2 the receiving mechanism is further configured to receive an authentication
3 credential from the user, the apparatus further comprising:
4 a verifying mechanism that is configured to verify that the authentication
5 credential is valid; and
6 a time-stamp mechanism that is configured to provide the time-stamped
7 token to the user-device, wherein the time-stamped token includes the
8 authentication and a time.

1 21. (Original) The apparatus of claim 20, further comprising:

2 a recovering mechanism that is configured to recover the time-stamped
3 token from the user-device;
4 an adding mechanism that is configured to produce the specified period to
5 the time within the time-stamped token to produce an expiry time; and
6 a detecting mechanism that is configured to detect if a current time is later
7 than the expiry time, whereby if the current time is later than the expiry time, the
8 authentication has expired.

1 22. (Original) The apparatus of claim 21, wherein the time within the
2 time-stamped token is updated to the current time by a partner application when
3 the partner application is accessed.

1 23. (Original) The apparatus of claim 20, wherein the time-stamped
2 token is a domain cookie, wherein the domain cookie is accessible by multiple
3 network servers within a domain on the public network.

1 24. (Original) The apparatus of claim 20, wherein the time-stamped
2 token is encrypted to prevent attacks.